Initial Concept for Commonwealth of Virginia Cyber Information Exchange and Reporting Portal

Commonwealth of Virginia Cyber Commission

Public Awareness and Culture Work Group

Initial work group activities have identified the need for enhanced cyber information exchange to counties, municipalities, small to mid-sized businesses, and citizens. We initially define cyber information exchange as providing cyber threat information, recommended actions and best practices, processing and channeling requests for additional information or assistance, and providing a reporting location for suspected cyber incidents.

There is a broad range of these types of information exchanges occurring between Federal cyber entities, State, and large businesses (especially those operating Critical Infrastructure); to varying degrees, these entities have made investments (both $ and personnel) to participate in collaborative forums to enhance their overall cyber readiness. Figure 1 provides a very simplistic view of existing information flows and collaboration between the Federal level, the States, and the major private and public organizations operating within State boundaries.

The work group believes that there is a significant gap in providing this type of Cyber information exchange down to the regional and local levels. There are numerous reasons for this gap; cities and counties are unable to generate the resources needed to develop cyber trained personnel to access the broad information available at the federal levels and even if they did, would be challenged to provide their leadership with explanations of what it means for their community. Small and mid-sized businesses also face the same resource challenges and ability to fully comprehend the threat and what they should be doing to protect themselves and their customers; weaknesses in these businesses also represents a supply chain threat to the larger businesses that they serve and supply as well a potential source for citizen PII. Commonwealth citizens also find it challenging to obtain clear, concise, and most importantly understandable information on how to reduce their overall cyber risk. All of these entities would be challenged to articulate how they would report a suspected cyber event in their area of responsibility or understand who might be able to assist them.

The work group has identified the need for a Cyber Information Exchange and Reporting Portal targeted to serve these constituent groups. A web based portal with capability to generate out of band alerting to information (text, e-mail, RSS feed, social media) is likely the best mechanism to interface with the broad constituent group. Existing systems like the Innovate VA platform or other Commonwealth web assets could likely be easily adapted for this use. The core need to establish this capability will be the analysts and communications specialist needed to 1) review the broad amount of information flowing down from the Federal and other cyber information feeds to 2) extract pertinent information for the constituent groups being served and 3) packaging this information into communications that can be easily comprehended by those receiving it and then 4) placing the information in the appropriate communications channel on the portal. Additionally, cyber E911 and 511 like operators would be required to screen reports of cyber incidents and requests for information to channel them to the appropriate response or assistance channel. Existing Commonwealth call center systems could likely be adapted for these purposes.

This concept aligns well with the Joint Cyber Operations Group concept that is being developed within the Cyber Infrastructure and Commonwealth Network Protection work group. We envision that the analysts, portal operators, and call center personnel would be co-located with the other Commonwealth, Federal, and private sector entities to provide a “unity of effort” approach. Collocation significantly simplifies communication and collaboration, enhances cyber workforce development and provides career growth paths (i.e. start as a call center operator, grow to analyst, then assign to COV Security Operation Center).

An initial rough order of magnitude to establish this capability is listed below.

Initial Operating Capability (core business hour availability):

4 Cyber Analysts (one for each constituent group and one trainee).

2 Communications Specialists (to work with analysts to tailor product for constituent groups).

2 Cyber 911/511 operators to intake and process calls, web submissions, and e-mails.

1.5 FTE for Portal operations and maintenance especially if existing COV resource was leveraged.

1 managerial position for supervisory functions and representation/participation with Joint Cyber Operations Group (would report directly to JCOG lead).

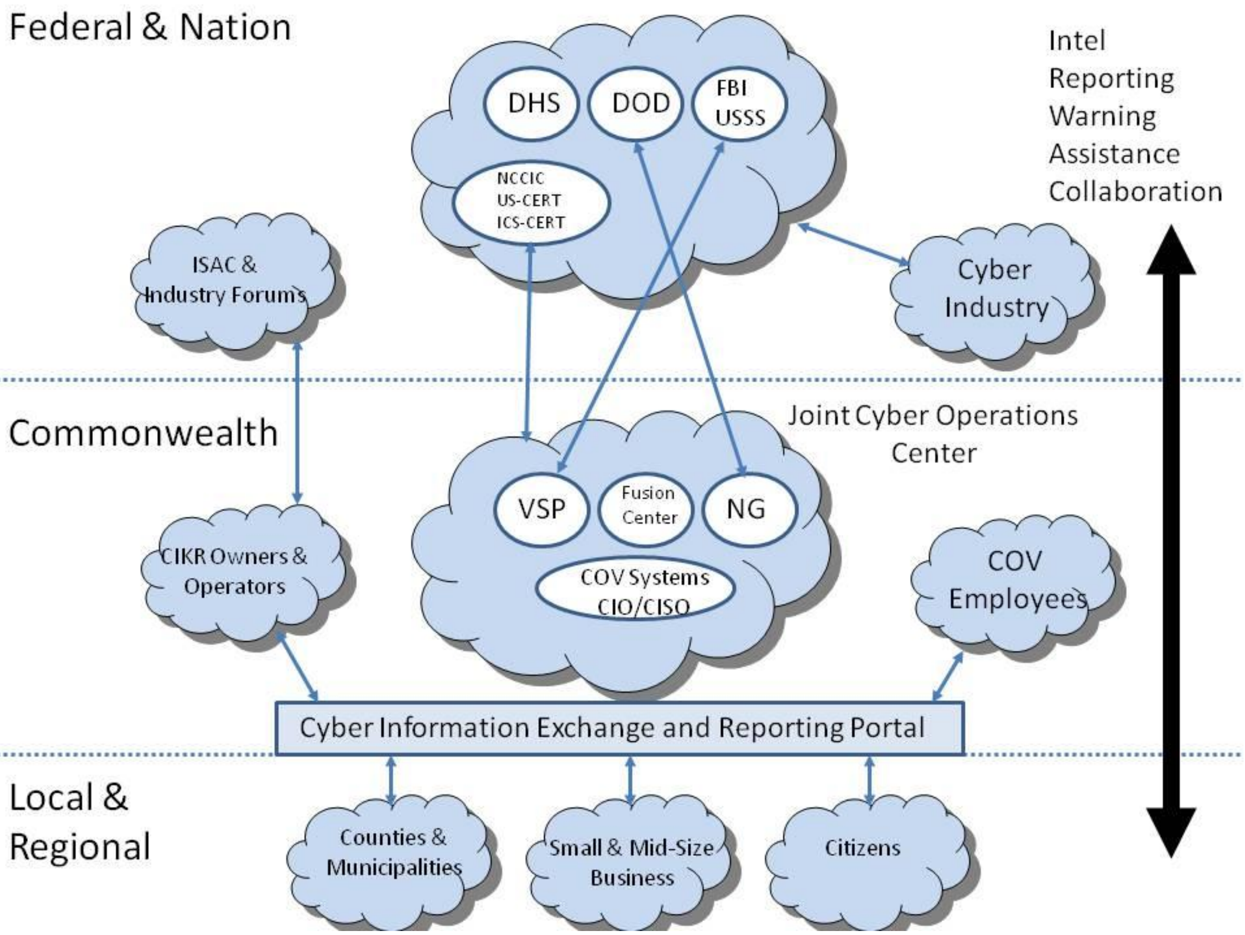
It would be expected that the analysts and communications specialists would spend several days a month doing outreach and interaction with the constituent groups they serve to continue to refine their products.

Full Operating Capability (24x7 availability):

6 Cyber Analysts, 3 Communication specialists, 4 911/511 operators, 1.5 FTE for portal operations, 1 manager and 1 deputy manager.

Portal and call center costs dependent on potential reuse of existing COV systems.

Figure 1.


Federal & Nation
DHS
DOD
FBI
USSS
NCCIC
US-CERT
ICS-CERT
Intel
Reporting
Warning
Assistance
Collaboration
ISAC &
Industry Forums
Cyber
Industry
Commonwealth
Joint Cyber Operations
Center
VSP
Fusion
Center
NG
COV Systems
CIO/CISO
CIKR Owners &
Operators
COV
Employees
Cyber Information Exchange and Reporting Portal
Local &
Regional
Counties &
Municipalities
Small & Mid-Size
Business
Citizens